Arithmétique et Théorie des Nombres pour la Cryptographie

TD 6. Formes quadratiques

Exercice 1
On considère une forme quadratique binaire $q(x,y) = ax^2 + bxy + cy^2$, et la matrice $Q = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ associée. Noter que Q n'est pas nécessairement à cœfficients entiers (si b est impair). On désigne par M^T la transposée d'une matrice M.

a) Vérifier que pour tous $x, y \in \mathbb{Z}$, on a

$$q(x,y) = \begin{pmatrix} x \\ y \end{pmatrix}^T Q \begin{pmatrix} x \\ y \end{pmatrix} \quad .$$

b) Pour $A = \begin{pmatrix} p & r \\ s & t \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, on note $q \cdot A$ la forme quadratique définie par $(q \cdot A)(x,y) = q(px + ry, sx + ty)$. Montrer que la matrice associée à $q \cdot A$ est $A^T Q A$.

c) Calculer les matrices associées à $q \cdot S$ et $q \cdot T_\lambda$, où $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et, pour $\lambda \in \mathbb{Z}$, $T_\lambda = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$.

Exercice 2
Calculer les discriminants des formes quadratiques :

$$52x^2 - 66xy + 21y^2 \ , \quad 27x^2 + 40xy + 15y^2$$

et donner à l'aide de l'algorithme vu en cours les formes quadratiques réduites correspondantes.

Exercice 3
On rappelle que, si $q(x,y) = ax^2 + bxy + cy^2$ est une forme quadratique imaginaire positive réduite (c'est-à-dire $D = b^2 - 4ac < 0$, $a > 0$, $|b| \leq a \leq c$ et $b \geq 0$ si $|b| = a$ ou $a = c$), on a : $a \leq \sqrt{-D/3}$.

a) Montrer qu'on a de plus :

$$\frac{-D}{4a} \leq c \leq \frac{a^2 - D}{4a} \quad .$$

b) Calculer le nombre $h(D)$ de classes d'équivalence de formes quadratiques primitives positives de discriminant D pour $D \in \{-4, -8, -12, -20, -39, -67\}$. Déterminer un représentant de chaque classe.

On connaît la liste des discrimants fondamentaux $D < 0$ tels que $h(D) = 1$:

$$\{-3, -4, -8, -7, -11, -19, -43, -67, -163\} \ .$$

Noter que -12 n'est pas un discriminant fondamental ($-12/4 = -3 \equiv 1 \mod 4$), ce qui explique qu'on ait pu trouver une forme quadratique non primitive de discriminant -12.

Exercice 4
Soient p un premier impair, D un entier non carré congru à 0 ou 1 modulo 4, avec $(D, p) = 1$.

1. a) Montrer qu'une forme quadratique représente proprement p si et seulement si elle le représente (tout court).
   b) En déduire que si une forme quadratique q de discriminant D représente p, alors $\left(\frac{D}{p}\right) = 1$.
2. On suppose que $\left(\frac{D}{p}\right) = 1$.
   a) Montrer qu'il existe un entier b tel que $D \equiv b^2 \mod p$ et que, quitte à le remplacer éventuellement par $b + p$, on aura aussi $D \equiv b^2 \mod 2$;
   b) montrer en utilisant l'hypothèse $D \equiv 0$ ou $1 \mod 4$ qu'on a de plus $D \equiv b^2 \mod 4$;
   c) en déduire que $D \equiv b^2 \mod 4p$, puis qu'il existe une forme quadratique q de discriminant D qui représente p.
3. Conclusion ?

Exercice 5
Pour n entier ≥ 1, on note q_n la forme quadratique définie par $q_n(x, y) = x^2 + ny^2$, de discriminant $D_n = -4n$.

1. On considère le cas $n \in \{1, 2, 3\}$.
   a) Montrer à l'aide de l'exercice 3 que pour $n \in \{1, 2, 3\}$, un premier impair p est représenté par une forme quadratique de discriminant $-4n$ si et seulement si il est représenté par q_n. Qu'en est-il pour 2 ?
   b) En déduire à l'aide de l'exercice 4 quels nombres premiers sont représentés par q_1 ; faire de même avec q_2 et q_3.
2. On considère le cas $n = 5$.
   a) Vérifier que D_5 est un discriminant fondamental. Il s'ensuit que toutes les formes quadratiques de discriminant D_5 sont primitives.
   b) Montrer qu'un nombre premier p vérifie $\left(\frac{-5}{p}\right) = 1$ si et seulement si p est congru à 1, 3, 7 ou 9 modulo 20.
   c) Comme $h(-20) = 2$, tous ces premiers ne sont pas nécessairement représentés par q_5 ; vérifier que $x^2 + 5y^2$ n'est jamais congru à -1 modulo 4, tandis que $2x^2 + 2xy + 3y^2$ n'est jamais congru à 1 modulo 4 ;
   d) en déduire quels nombres premiers sont représentés par q_5, respectivement par la forme quadratique $2x^2 + 2xy + 3y^2$.
3. Loi de composition pour $n = 5$.
   a) Vérifier que le raisonnement tenu dans l'exercice précédent permet de montrer, pour n entier impair et D entier non carré congru à 0 ou 1 modulo 4 avec $(D, n) = 1$, l'équivalence des deux assertions suivantes :
      (i) il existe q de discriminant D qui représente proprement n ;
      (ii) D est un carré modulo n.
   b) Soit $n = pp'$ un entier produit de deux nombres premiers impairs distincts de 5. Établir que D_5 est un carré modulo n si et seulement si $\left(\frac{-5}{p}\right) = \left(\frac{-5}{p'}\right) = 1$.
   c) En déduire que si p, p' sont congrus à 3 ou 7 modulo 20, alors n est représenté par q_5 ; ceci peut-il s'expliquer grâce à l'égalité suivante (due à Lagrange) ?

$$(2x^2 + 2xy + 3y^2)(2z^2 + 2zw + 3w^2) = (2xz + xw + yz + 3yw)^2 + 5(xw - yz)^2 \; .$$